49 98

CLAIMS

1. A method of monitoring client-usage of digital content provided by a content provider (30) to a client system (10) over a network (40), said method including the step of:

- logging information concerning the actual rendering of said digital content individually for each rendering to be monitored; and
- performing a security operation to enable identification of at least one of an account and an individual for linking said usage information thereto.

2. The method according to claim 1, further comprising the step of decrypting said digital content prior the rendering of said digital content.

3. The method according to claim 1, wherein said step of performing a security operation comprises the step of performing at least part of an authentication of said information.

4. The method according to claim 1, wherein said information is maintained in a log (175) in said client system (10), and said step of performing a security operation comprises the step of storing said log (175) in a tamper-resistant environment associated with said client system (10).

5. The method according to claim 1, wherein said information comprises a representation (172-1) of said client-rendered digital content and rendering quality information (172-2).

6. The method according to claim 5, wherein said quality information (172-2) comprises at least one of:

- bandwidth of said rendered digital content;
- sample rate of said digital content;

- data compression of said digital content;
- resolution of said used digital content;
- time information (172-N) related to rendering of said digital content; and
- information of any disruptions during the rendering of said digital content.

7. The method according to claim 1, wherein said information comprises at least one of:

- identification of a content-usage device (300);
- information on payment of said digital content;
- time information (172-N) related to rendering of said digital content;
- time information related to transmittal of said digital content from said content provider (30) to said client system (10); and
- time information related to reception of said digital content by said client system (10).

8. The method according to claim 1, wherein said logging step comprises the steps of:

- tamper-resistantly generating said information; and
- storing said information as a log entry (172) in a user-tamper-resistant log (170; 175; 175-1, 175-2).

9. The method according to claim 1, wherein said logging step comprises the step of generating said information during said digital content rendering or after said digital content rendering.

10. The method according to claim 1, further comprising the step of forwarding said information from said client system (10) to an external trusted party for storage therein as log entry (172) in a usage log (170).

51 50

ART 34 AMDT

11. The method according to claim 1, wherein said digital content is provided as streaming data and said digital data is used by said client system (10), said step of logging information comprises the step of for each on-going client-usage of streaming data, intermittently logging information during said client-usage.

12. The method according to claim 11, further comprising the step of intermittently forwarding said intermittently logged information to said content provider (30) for confirming reception and rendering of the data.

13. The method according to claim 12, wherein said information is included into receive reports associated with the report mechanism of the streaming protocol used for streaming said data.

14. Client system (10) capable of using digital content provided by a content provider (30) over a network (40), said content-using client system (10) comprising:

- logging agent (150) for logging information concerning the actual rendering of said digital content individually for each one of a set of client-renderings; and
- means (160; 460) for performing a security operation to enable identification of at least one of an account and an individual for linking said information thereto.

15. The client system according to claim 14, further comprising means (130; 430) for decrypting said digital content prior the rendering of said digital content.

16. The client system according to claim 14, wherein said security operation performing means (160; 460) is configured for performing at least part of an authentication of said information.

17. The client system according to claim 14, wherein said information is maintained in a log (175) in said client system (10), and said security operation

performing means is configured for storing said log (175) in a tamper-resistant environment associated with said client system (10).

18. The client system according to claim 14, wherein said information comprises a representation (172-1) of said client-rendered digital content and rendering quality information (172-2).

19. The client system according to claim 14, wherein said logging agent (150) comprises:

- means (152) for tamper-resistantly generating said information; and
- means (154; 156) for storing said information as a log entry (172) in a log (170; 175).

20. The client system according to claim 14, wherein said logging agent (150) comprises means (152) for generating said information during or after rendering of said digital content.

21. The client system according to claim 14, wherein said logging agent (175) further comprises means (156) for forwarding said information to an external trusted party for storage therein as a log entry (172) in a log (170).

22. The client system according to claim 14, further comprising:

- a rendering device (300) adapted for rendering said provided digital content; and
- a first digital rights management (DRM) agent (130; 330), at least partly implemented in said rendering device (300), having functionality for enabling rendering of said digital content.

23. The client system according to claim 22, further comprising:

- a second DRM agent (230; 430) implemented in said client system (100), having functionality for enabling reception of said digital content from said content provider (30); and

- means (210; 310; 410) for communication between said first DRM agent (330) and said second DRM agent (230; 430), said first DRM agent (330) comprising means for transferring a first control signal associated with said information to said second DRM agent (230; 430) and said second DRM agent (230; 430) comprises means for processing signal data associated with said first control signal to generate a second control signal, and means for sending said second control signal to said first DRM agent (330) for controlling the digital-content usage process.

24. The client system according to claim 14, further comprising a tamper resistant module, in which said logging agent (150) is implemented.

25. The client system according to claim 24, wherein said tamper resistant module is a subscriber identity module (400).

26. The client system according to claim 25, wherein said logging agent (150) is at least partly implemented as an application in an application environment (490) provided by an application toolkit associated with said subscriber identity module (400).

27. The client system according to claim 26, wherein said logging agent application is downloaded into said subscriber identity module (400) over said network (40) from a network service provider (20; 30) associated with said subscriber identity module (400).

28. The client system according to claim 14, wherein said digital content is provided as streaming data and said client system (10) comprises means (300) for rendering said streaming data, and said logging agent (150) is configured to, for each

on-going client-rendering of streaming data, intermittently generate information during said client-rendering.

29. The client system according to claim 28, further comprising means (156) for intermittently forwarding said intermittently generated information to said content provider (30) for confirming reception and rendering of the data.

30. The client system according to claim 29, wherein said information is included into receive reports associated with the report mechanism of the streaming protocol used for streaming said data.

31. A digital rights management system for assisting in the management of digital content provided to a client system (10) over a network (40), said management system comprising:

- means (22) for receiving, for each one of a set of renderings of said digital content by said client system (10), information over said network (40), said information concerning the rendering of said digital content and originating from said client system (10); and
- means (180) for storing said information in a log (170; 175)), said information being subjected to at least part of an authentication procedure to enable identification of at least one of an account and an individual for linking said information thereto.

32. The system according to claim 31, further comprising means (22) for downloading a logging agent (150) into said client system (10), said logging agent (150) being operable, when executed in said client system (10), for generating, for each one of said client-renderings, information concerning the rendering of said digital content and forwarding said information to said storing means (180).

33. The system according to claim 31, wherein said digital content providing means (32) is configured for providing said digital content to said client system (10) as streaming data, said system further comprising means (32) for terminating the flow of streaming data to said client system (10) if no information has been received during a predetermined period of time.

34. The system according to claim 31, wherein said system is implemented in a network operator node.

35. A tamper-resistant device (400) adapted for cooperation with a client system (10) capable of rendering digital content provided by a content provider (30) over a network (40), said tamper-resistant device (400) comprising:

- logging agent (150) for logging information concerning the rendering of said digital content individually for each one of a set of client-renderings, said tamper-resistant device (400) being associated with means (160; 460) for performing a security operation to enable identification of at least one of an account and an individual for linking said information thereto.

36. The device according to claim 35, further comprising means (430) for decrypting said digital content prior to the rendering of said digital content.

37. The device according to claim 35, wherein said security operation performing means (160; 460) is provided in said tamper-resistant device (400) for performing at least part of authentication of said information.

38. The device according to claim 35, wherein said information is maintained in a log (175) in said tamper-resistant device (400).

56 55

39. The device according to claim 35, wherein said logging agent (150) comprises means (152) for generating said information during or after rendering of said digital content.

40. The device according to claim 35, wherein said logging agent (150) further comprises means (156) for forwarding said information to an external trusted party for storage therein as a log entry (172) in a log (170).

41. The device according to claim 35, wherein said tamper-resistant device (400) is a subscriber identity module.

42. The device according to claim 41, wherein said logging agent (150) is at least partly implemented as an application in an application environment (490) provided by an application toolkit associated with said subscriber identity module (400).

43. The device according to claim 35, wherein said logging agent application is downloaded into said subscriber identity module (400) over said network (40) from a network service provider (20; 30) associated with said subscriber identity module (400).

44. The device according to claim 35, further comprising means for downloading upgrades of said logging agent (150).

45. A method of monitoring client-usage of a service provided by a service provider (30) to a client system (10), said method including the step of:

- logging usage information concerning the actual usage of said service individually for each usage to be monitored; and
- performing a security operation to enable identification of at least one of an account and an individual for linking said usage information thereto.